SIR IUS 5/22
SLOVENSKI INŠTITUT za REVIZIJO
Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

Kazalo

Iz prakse za prakso

Bonitetni nadzor

Alternativni investicijski skladi in ocenjevanje njihovih naložb za ugotavljanje čiste vrednosti sredstev AIS-ov

Nenačrtovani notranjerevizijski posli

Začetna bilanca stanja samostojnega podjetnika ob spremembi načina obdavčitve v upoštevanje dejanskih prihodkov in dejanskih odhodkov

Neposlovna raba pri električnih vozilih, kadar DDV ni bil odbit

Novosti in obvestila

Novi nazivi

Mag. Maja Hmelak

Revizija upravljanja dostopnih pravic – ključne teme v letu 2022

Auditing User Access Privileges – key issues in 2022

Povzetek • *Ustrezno upravljan dostop do informacijskih virov je ključni pogoj za učinkovito in varno delo, zato je to področje pogosto predmet revizijskih pregledov. Temo dostopnih pravic smo v reviji SIR*IUS že večkrat obravnavali. Pogoste tehnološke in druge spremembe pa zahtevajo, da revizijski pristop nenehno prilagajamo in razširjamo. V pričujočem prispevku nadgrajujemo pretekle prispevke. Pripravili smo pregled področja in predlagamo možen praktični pristop k njegovi reviziji s poudarki na temah, ki so za to področje v letu 2022 še posebej aktualne – nove grožnje zlorabe dostopnih pravic, novi standardi in novi tehnološki pristopi k zmanjševanju tveganj.*

Prispevek je pripravljen predvsem za revizorje, ki niso strokovnjaki za informacijske tehnologije, saj vsebuje vrsto opredelitev temeljih pojmov področja. Poleg tega obravnava tudi nove trende področja dostopnih pravic. Namen prispevka je, da se spodbudi čim več revizij tega področja, saj je velik del področja upravljanja dostopnih pravic tehnično manj zahteven in ga lahko izvedejo tudi osebe z omejenim tehnološkim znanjem.

Ključne besede • *uporabniški dostopi, kibernetska varnost, spletna varnost, NIS, CER, vdor, razkritje podatkov, nič-zaupanja*

Summary • *Appropriately managing of user access privileges is crucial in ensuring efficient and safe work environment. The area of user access management is therefore frequently subject to auditing and had also been a subject of several SIR*IUS articles. Although we have published articles on this subject before, technical and other changes require continuous evolvement of our audit approach. In this article, we propose a practical approach to user access management audit with emphasis on key issues in 2022 – new threats to user access, new standards and new tools to reduce its inherent risks.*

The article was primarily written for auditors, who do not have an IT audit background. As many aspects of user access management audits can be performed without advanced technical skills, the author hopes, that this approach will encourage such auditors, to undertake this type of audit as the area is of increasing importance.

Key words • *user access, cyber security, NIS, CER, breach, data leak, zero-trust*

Gašper Krajnc

Posli dajanja zagotovil, vezani na storitvene organizacije, in poročila SOC® o kontrolah nad informacijami in sistemi storitvene organizacije

Assurance engagements at a service organization and System and Organization Control reports (SOC) with focus on SOC 2 report

Povzetek • *V prispevku so opisani revizijski posli dajanja zagotovil SOC (System and Organization Control) in poročila o kontrolah nad informacijami in sistemi storitvene organizacije (SOC reports), ki se nanašajo na notranje kontrole storitvene organizacije ali njene sisteme. Osredotočamo se na revizijski posel in poročilo vrste SOC 2. Navajamo standarde, po katerih revizor storitvene organizacije poroča, in standarde, po katerih presoja obravnavano zadevo, ter opisujemo možnosti in koristi uporabe poročila SOC 2.*

Ključne besede • *zagotovilo, dajanje zagotovil, storitvena organizacija, kontrole, informacije, sistemi, informacijski sistem, SOC, SOC 1, SOC 2, kriteriji zaupanja, kibernetska varnost, kibernetska tveganja v dobavnih verigah, MSZ 3000, COSO, AICPA*

Summary • *In this paper, we introduce reasonable assurance engagements and reports on controls at a service organisation based on SOC (System and Organization Control). Specifically, we dive into SOC 2 report on the description, design (and operating effectiveness) of controls at a service organization. We list the standards according to which the auditor reports as well as applicable criteria. Finally, we briefly describe the benefits and use of a SOC 2 report.*

Key words • *assurance, service organization, controls, information, systems, Service Organization Controls, SOC, SOC 1, SOC 2, System and Organizations control reports, Trust Service Criteria, cyber security, supply chain cyber security, ISAE 3000, COSO, AICPA*

Mag. Aleksandra Plahuta

Revizija neprekinjenega poslovanja

Business Continuity Audit

Povzetek • *Nepričakovani dogodki, kot so naravne nesreče, epidemije in pandemije, kibernetski napadi, izpadi električne energije ali internetne povezave, okvare informacijskega sistema ali infrastrukture in podobno, lahko resno ogrozijo obstoj organizacije. Zato sta ključnega pomena pripravljenost in ustrezen sistem, ki zagotavlja neprekinjeno poslovanje. Organizacije, ki želijo ustrezno obvladovati tveganja in imajo vpeljan sistem upravljanja neprekinjenega poslovanja ali načrtujejo vpeljavo takega sistema, lahko preverijo stanje s presojami in analizami, pa tudi z revizijskim pregledom. V prispevku je predstavljen pristop k reviziji neprekinjenega poslovanja in dajanju zagotovil učinkovitosti neprekinjenega poslovanja javne organizacije, ki smo ga že večkrat izvedli na Računskem sodišču Republike Slovenije.*

Ključne besede • *neprekinjeno poslovanje, neprekinjeno delovanje, revizija neprekinjenega poslovanja, sistem upravljanja neprekinjenega poslovanja, informacijski sistem*

Summary • *Unexpected events such as natural disasters, epidemics and pandemics, cyber attacks, power outages or internet disruptions, information system or infrastructure failures etc. can seriously endangere the existence of the organization. Thus, security preparedness and an appropriate system to ensure business continuity are of crucial importance. Organizations that have appropriate risk management, where applicable, and also have in place or plan to implement a business continuity management can verify the situation through checks and analyses, as well as audits. The paper presents an approach to the audit of business continuity and to providing the assurance of the efficient business continuity of a public organization, which has been carried out several times at the Court of Audit of the Republic of Slovenia and is described in more detail in this paper.*

Key words • *business continuity, continuous operation, business contiunuty audit, business continuity management system, information system*

Ruti Rous

Oblikovanje dogovorov o zagotavljanju ravni informacijskih storitev

Drafting Service level agreements

Povzetek • *V času, ko se informacijske rešitve čedalje pogosteje ponujajo v obliki storitev, se povečuje tudi potreba po ustrezni pravni ureditvi razmerij med ponudnikom in uporabnikom informacijskih storitev. Pri tem je treba upoštevati specifične dejavnike in tveganja, ki izhajajo zlasti iz naraščajoče odvisnosti poslovnih procesov od dostopnosti informacijskih storitev, občutljivosti informacijskih storitev na varnostne incidente ter potreb po varovanju osebnih in drugih občutljivih podatkov, ki so vključeni v izvajanje storitve. Zato je ključno, da ponudnik in uporabnik skleneta ustrezen dogovor o zagotavljanju ravni informacijskih storitev.*

Glede na to, da so cene informacijskih storitev lahko visoke, predvsem pa je lahko visoka škoda, ki preti organizaciji ob morebitnem nedelovanju informacijske podpore ključnim poslovnim procesom, menim, da bi morala biti dogovorom o zagotavljanju ravni storitve tako pri sklepanju kot pri revidiranju posvečena posebna pozornost.

V članku so predstavljene temeljne pravne podlage in osnovni elementi, ki jih je treba upoštevati pri presoji, kaj bi moralo biti vključeno v tovrstni dogovor. Pri tem opozarjam, da bi oblikovanje dogovorov moralo temeljiti na vsakokratni individualni analizi tveganj.

Ključne besede • *SLA, dogovor, informacijske storitve, zagotavljanje ravni, varstvo osebnih podatkov, vsebina pogodbe*

Summary • *In a time when application software is increasingly being offered as a service, the need for a formalized legal relationship between a service provider and a service user increases accordingly. While drafting these provisions some specific factors need to be taken into consideration, with special emphasis on the risks deriving from software dependency of a business process, software sensibility on cybersecurity incidents, and the need for protection of data being processed in the delivery of a service. Therefore, a proper legal agreement between the service provider and the user of the service is essential.*

In my opinion, concerning the cost of application software service and the potential damages threatening the organization in the event of service unavailability, a

service level agreement should be drafted and audited with particular vigilance. In this article, I present main legal provisions and elements that need to be considered while drafting service level agreements. However, I suggest individual service risk analysis is fundamental for drafting a service level agreement.

Key words • *SLA, agreement, service level, software as a service*

Dušan Hartman

Koncept pomembnosti z računovodskega in revizijskega vidika

Concept of materiality from accounting and auditing prospective

Povzetek • *V prispevku je prikazan koncept pomembnosti, kot ga opredeljujejo Mednarodni standardi računovodskega poročanja/Slovenski računovodski standardi ter Mednarodni standardi revidiranja. Določanje pomembnosti je ključno pri delu računovodje in revizorja. Sam pojem pomembnosti celote računovodskih izkazov je tako z računovodskega kot z revizijskega vidika zelo podoben. Z revizijskega vidika pa se pojem pomembnosti celote računovodskih izkazov razširi še na izvedbeno pomembnost, ki je ključna za revidiranje računovodskih izkazov. Na koncu prispevka je računovodjem in revizorjem namenjenih tudi nekaj praktičnih napotkov za uporabo pomembnosti*

Ključne besede • *pomembnost celote računovodskih izkazov, izvedbena pomembnost, MSRP/MRS, SRS, MSR, računovodja, revizor*

Summary • *This article will present the concept of materiality as defined by IFRS/SAS and International Standards on Auditing. Determining materiality is of key importance in the work of accountants and auditors. The very concept of materiality of financial statements as a whole is very similar from both an accounting and an auditing perspective. From the auditing perspective, the concept of materiality of financial statements as a whole is extended to the materiality of implementation, which is a key issue for the audit of financial statements. The final part of the article will include some practical guidelines on the use of materiality for accountants and auditors.*

Key words • *materiality of financial statements as a whole, performance materiality, IFRS/IAS, SAS, IAS, accountant, auditor*